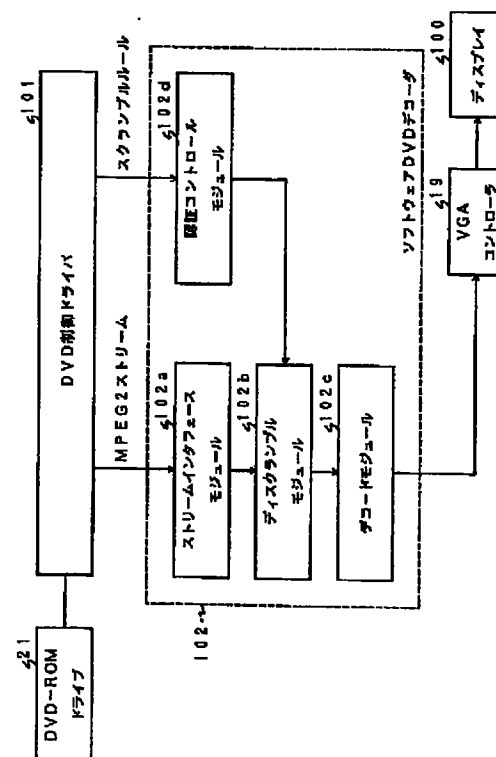


(11)特許出願公開番号



【特許請求の範囲】

【請求項1】 フレーム内符号化画像およびフレーム間予測符号化画像を含むデジタル圧縮符号化された動画データに対して暗号化処理を施して、その動画データの不正使用を防止する動画像データ暗号化方法において、前記デジタル圧縮符号化された動画データの中で前記フレーム内符号化画像に対してのみ暗号化処理を施し、前記動画データの一部についてのみの暗号化によって動画データの不正な表示再生を防止できるようにしたことを特徴とする動画像データの暗号化方法。

【請求項2】 前記フレーム内符号化画像に対する暗号化処理は、前記フレーム内符号化画像を所定のルールで演算するスクランブル処理によって実行されることを特徴とする請求項1記載の暗号化方法。

【請求項3】 前記スクランブル処理されたフレーム内符号化画像を含む動画像データは、リードインエリア、プログラムエリア、およびリードアウトエリアから構成されるデータ列のプログラムエリアとして光ディスクに蓄積され、前記リードインエリアには、前記スクランブル処理のための演算ルールを示すスクランブルルール情報が格納されており、前記光ディスクから前記プログラムエリアの動画データを読み出し、その動画データに含まれるフレーム内符号化画像に対してその逆スクランブルのための演算処理を前記スクランブルルール情報に基づいて実行した後、動画データの復号を行うことを特徴とする請求項2記載の暗号化方法。

【請求項4】 前記動画データのデータ列は、ヘッダ部とデータ部とから構成されており、前記ヘッダ部には、前記暗号化処理されたフレーム内符号化画像の位置を示す情報が含まれていることを特徴とする請求項1記載の暗号化方法。

【請求項5】 動画像をデジタル圧縮符号化し、フレーム内符号化画像およびフレーム間予測符号化画像を生成する動画像符号化手段と、この動画像符号化手段で符号化されたフレーム内符号化画像に対して暗号化処理を施す手段とを具備し、前記動画データの一部についてのみの暗号化によって動画データの不正使用を防止できるようにしたことを特徴とする動画像符号化装置。

【請求項6】 フレーム内符号化画像およびフレーム間予測符号化画像を含むデジタル圧縮符号化された動画像データを復号する動画像復号装置において、前記デジタル圧縮符号化された動画像データから暗号化処理されたフレーム内符号化画像を抽出し、その暗号化されたフレーム内符号化画像を解読する手段を具備することを特徴とする動画像復号化装置。

【請求項7】 CPUと、デジタル圧縮符号化された動

画データが蓄積された蓄積メディアからデータを読み出すためのディスクドライブ装置を制御可能なディスクインターフェースとを備え、前記デジタル圧縮符号化された動画像データの復号及び再生が可能なコンピュータシステムにおいて、

前記CPUに、前記ディスクインターフェースを介して前記ディスクドライブ装置から読み出される動画データの中から暗号化処理されたフレーム内符号化画像を抽出させる手段と、

前記CPUに、その抽出されたフレーム内符号化画像の解読処理を実行させる手段とを具備することを特徴とするコンピュータシステム。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】 この発明は動画像データの暗号化方法およびその方法が適用されるコンピュータシステム並びに動画像データ符号化／復号化装置に関する。

【0002】

【従来の技術】 近年、コンピュータ技術の発達に伴い、いわゆるマルチメディア対応のパーソナルコンピュータが種々開発されている。この種のパーソナルコンピュータでは、テキストデータやグラフィックスデータの他に、動画や音声データを再生することができる。

【0003】 通常、動画データはMPEG1によって圧縮符号化されてCD (Compact Disk) などに記憶されており、その動画データのデコードおよび表示再生には、専用の拡張ボードが使用されている。動画データのデコードおよび表示再生を行う拡張ボードとしては、例えば、米シグマデザイン社の“REAL Magic”が良く知られている。この“REAL Magic”は、MPEG1の規格に準拠したビデオデコード機能を有しており、デコードされた動画データは、フィーチャコネクタを介してビデオカードから取り込まれたVGAグラフィックスと合成されて表示される。

【0004】 しかし、MPEG1の規格は、1.5Mbps程度のデータ転送速度を持つCDを使用することを前提とした規格であり、映画などの大量の画像情報を含む動画データを扱うと、画質の劣化などの問題が生じる。

【0005】 そこで、最近では、CDの数倍乃至十数倍程度のデータ転送速度を持つ新世代の蓄積メディアとしてDVD (Digital Versatile Disk) が開発されている。DVDはMPEG2という動画像符号化を使って、CDと同じ大きさの光ディスクに、映画などの映像情報を高画質で記録できる新しいビデオディスク規格である。DVDの記録再生方法は、画質と、容量に対する記録時間の双方を確保する観点から、可変レート符号化の考えに基づいている。可変レート符号化データのデータ量は、元の画像の画質に依存し、動きの激しいシーンほどそのデータ量は増加する。

【0006】このDVDに蓄積された動画データをパーソナルコンピュータ上で再生する場合には、DVD-ROMからコンピュータの主記憶にデータが読み込まれ、そしてそれがDVDデコーダに転送されることになる。この場合、主記憶に読み込まれたデータの不正コピー、およびその不正使用を防止するためには、動画データに含まれるすべての映像情報に対してスクランブル処理などの暗号化を施すことが必要となる。

【0007】ところで、近年のCPUの高速化により、専用のハードウェアによって動画データをデコードするのではなく、ソフトウェアによって動画データをデコードするという、いわゆるソフトウェアデコーダの実現が望まれている。ソフトウェアデコーダによって動画データをデコードすることにより、専用のハードウェアが不要となり、システム全体のコストを低減することが可能となる。

【0008】しかし、ソフトウェアデコーダを使用した場合には、MPEG2で符号化された動画データを復号するという本来の処理のみならず、それに先だって、スクランブル処理された動画データを元に戻すというディスクランブル処理についてもCPUによって実行することが必要とされる。ディスクランブル処理の対象となるのは動画データに含まれるすべての映像情報であるため、それに要するCPUの負荷はかなり大きい。従って、CPUパワーの多くがディスクランブル処理に取られてしまい、リアルタイムにデコード処理を行うことは実際上困難である。

【0009】

【発明が解決しようとする課題】上述したように、従来では、映像情報すべてをスクランブルしているため、そのディスクランブル処理のために多くのCPUパワーが必要とされる。したがって、コピープロテクト機能とソフトウェアデコーダとを同時に満足することは実際上困難であった。

【0010】この発明はこのような点に鑑みてなされたものであり、動画データの一部のみを暗号化するだけでその動画データの表示再生などの不正使用を防止できるようにし、コピープロテクト機能とソフトウェアデコーダとを同時に満足させることが可能な動画像データの暗号化方法およびその方法が適用されるコンピュータシステム並びに動画像データ符号化／復号化装置を提供することを目的とする。

【0011】

【課題を解決するための手段】この発明は、フレーム内符号化画像およびフレーム間予測符号化画像を含むデジタル圧縮符号化された動画データに対して暗号化処理を施して、その動画データの不正使用を防止する動画像データ暗号化方法において、前記デジタル圧縮符号化された動画データの中で前記フレーム内符号化画像に対してのみ暗号化処理を施し、前記動画データの一部について

のみの暗号化によって動画データの不正な表示再生を防止できるようにしたことを特徴とする。

【0012】この動画像データ暗号化方法においては、MPEG2などでデジタル圧縮符号化された動画データにおいては、フレーム内符号化画像（Iピクチャ）、片方向予測、双方向予測などのフレーム間予測符号化画像（Pピクチャ、Bピクチャ）が含まれているが、フレーム間予測符号化画像（Pピクチャ、Bピクチャ）の復号は、フレーム内符号化画像（Iピクチャ）を用いて行われており、フレーム内符号化画像（Iピクチャ）無しではフレーム間予測符号化画像（Pピクチャ、Bピクチャ）を正しく復号することができない点に着目し、フレーム内符号化画像（Iピクチャ）に対してのみスクランブル処理などによる暗号化を施したものである。

【0013】これにより、動画データに含まれるすべての画像情報に対してスクランブル処理を行うのではなく、動画データの一部についてのみのスクランブル処理で不正な表示再生を防止できるようになる。従って、ソフトウェアデコーダを利用する場合には、ディスクランブル処理のために要するCPUパワーを少なく抑制することが可能となり、動画データの復号処理をソフトウェアデコーダによってリアルタイムに行うことが可能となる。

【0014】

【発明の実施の形態】以下、図面を参照してこの発明の実施形態を説明する。図1には、この発明の一実施形態に係るコンピュータシステムで使用されるソフトウェアデコーダとその周辺のソフトウェア及びハードウェアの構成が示されている。DVD-ROMドライブ21は光ディスクから構成されるDVDメディアに蓄積されたビデオ、オーディオ、サブピクチャを含むMPEG2データストリームを読み出すためのものであり、DVDメディアに蓄積された動画データのストリームは図2のようなデータフォーマットを有している。

【0015】すなわち、データストリームは複数のセクタから構成されているが、動画データについては、各セクタは、図示のようにストリームヘッダ部とMPEG2データ部とから構成されている。MPEG2データ部には、MPEG2でデジタル圧縮符号化された画像、つまりIピクチャ、Pピクチャ、Bピクチャが含まれている。このうち、Iピクチャについてはその画像に対して所定の演算ルールでスクランブル処理が施されており、他のPピクチャ、Bピクチャについてはそのようなスクランブル処理は施されていない。ストリームヘッダ部には、スクランブル処理されている画像データの位置、つまりIピクチャの位置を示すスクランブル情報が含まれている。スクランブル情報については、暗号化処理を施しておいてもよい。このようなデータフォーマットでMPEG2データストリームを生成する符号化装置は、図4のように構成されている。

【0016】すなわち、図4に示されているように、符号化装置は、映画の主映像に相当するビデオデータをMPEG2でデジタル圧縮符号化するMPEG2エンコーダ501、オーディオ信号をドルビーAC3でデジタル圧縮符号化するオーディオエンコーダ502、および字幕などのサブピクチャをランレングス符号化などでデジタル圧縮符号化するサブピクチャエンコーダ503を備えている。MPEG2エンコーダ501で符号化されたビデオデータには、前述のIピクチャ、Pピクチャ、Bピクチャが含まれているが、IピクチャについてはIピクチャスクランブラ504によってビデオデータの中から抽出されてスクランブル処理が施される。そして、多重化回路505において、符号化されたビデオデータ、オーディオデータ、サブピクチャデータが一本のMPEG2プログラムストリームとして多重化されて、DVDメディアに蓄積される。

【0017】図1のDVD制御ドライバ101はDVD-ROMドライブ21からのMPEG2データの読み出しを制御するソフトウェアであり、動画再生時にMPEG2データをDVD-ROMドライブ21から読み出し、ソフトウェアDVDデコーダ102に渡す。このDVD制御ドライバ101はOSの一部として実現することもできる。

【0018】ソフトウェアDVDデコーダ102は、DVDメディアに蓄積されているMPEG2データを復号するためのものであり、図示のように、ストリームインタフェースモジュール102a、ディスクランブルモジュール102b、デコードモジュール102c、および認証モジュール102dから構成されている。ストリームインタフェースモジュール102aは、DVD制御ドライバ101を介して図2で説明したMPEG2データ部とスクランブル情報をDVD-ROMドライブ21から取得し、それをディスクランブルモジュール102bに渡す。

【0019】認証コントロールモジュール102dは、DVD制御ドライバ101を介してあるいは直接にDVD-ROMドライブ装置21と通信し、正当なソフトウェアモジュールであることをDVD-ROMドライブ装置21に通知するという認証処理を行う。そして、正当なソフトウェアモジュールであることが承認されると、DVD-ROMドライブ装置21からのスクランブルルールの読み出しが許可される。このスクランブルルール情報はIピクチャに対して施されたスクランブル処理の演算ルールを示すものであり、このスクランブルルール情報に対しても所定の暗号化処理が施されている。認証コントロールモジュール102dはスクランブルルール情報を解読し、それをディスクランブルモジュール102bに渡す。

【0020】スクランブルルール情報は、DVDメディアの最内周から最外周に渡る一本のデータ列の中で通常

のファイルシステムなどからはその読み出しができない位置、つまりリードインエリアに格納しておくことが好ましい。すなわち、光ディスクなどの蓄積媒体におけるデータ格納形式では、データは、図3に示されているようにリードインエリア、データエリア、リードアウトエリアから構成されているが、リードインエリアの内容は通常のファイルシステムから参照することはできない。このため、スクランブルルール情報をリードインエリアに格納しておくことにより、スクランブルルール情報が盗み見られることを防止することができる。

【0021】ディスクランブルモジュール102bは、MPEG2データ部に含まれるIピクチャの位置をスクランブル情報に基づいて特定し、MPEG2データ部からIピクチャを抽出する。そして、認証コントロールモジュール102dから得たスクランブルルール情報に基づいて、スクランブルされているIピクチャを元に戻すディスクランブル処理のための演算を実行する。

【0022】デコードモジュール102cは、MPEG2データを復号してそれを圧縮前の元の情報に伸張するものであり、ビデオデータのデコードだけでなく、サブピクチャおよびオーディオのデコードも行ふ。デコードされたビデオデータはデコードされたサブピクチャと合成されてVGAコントローラ19に送られ、ディスプレイ100に画面表示される。また、デコードされたオーディオデータはオーディオコントローラによって再生される。

【0023】次に、図5のフローチャートを参照して、動画再生処理の手順を説明する。動画データ再生用のアプリケーションプログラムから動画データの再生要求が発行されると、まず、認証コントロールモジュール102dがDVD-ROMドライブ21と通信してスクランブルルールを取得し、それを解読する（ステップS101）。次いで、ストリームインタフェースモジュール102aがMPEG2ストリームを取得し、スクランブル情報とMPEG2データをディスクランブルモジュールに渡す（ステップS102）。この時、必要に応じてスクランブル情報の解読も行われる（ステップS103）。スクランブル情報の解読はディスクランブルモジュール102bで行うことも可能である。

【0024】この後、ディスクランブルモジュール102bがMPEG2データに含まれるIピクチャの位置をスクランブル情報に基づいて特定し、認証コントロールモジュール102dから得たスクランブルルール情報に基づいてスクランブルされているIピクチャを元に戻すディスクランブル処理を実行する（ステップS104）。そして、デコードモジュール102cによってMPEG2データが復号がされ、動画及び音声の再生が行われる（ステップS105）。

【0025】以上のように、この実施形態においては、MPEG2データストリームにはフレーム内符号化され

たIピクチャ、片方向予測、双方向予測のフレーム間予測符号化されたPピクチャ、Bピクチャが含まれているが、Pピクチャ、Bピクチャの復号は、Iピクチャを用いて行われており、Iピクチャ無しではPピクチャ、Bピクチャを正しく復号することができない点に着目し、Iピクチャに対してのみスクランブル処理などによる暗号化を施している。これにより、すべての画像情報に対してスクランブル処理を行うのではなく、動画データの一部についてのみのスクランブル処理で不正な表示再生を防止できるようになる。従って、ディスクランブル処理のために要するCPUパワーを少なく抑制することが可能となり、動画データの復号処理をソフトウェアデコーダ102によってリアルタイムに行うことが可能となる。

【0026】また、専用のハードウェアデコーダを有するコンピュータシステムでは、ディスクランブル処理とデコード処理をハードウェアデコーダによって実行させることもできる。この場合、ディスクランブル処理はIピクチャに対してだけ行えばよいので、ディスクランブル処理のための回路は簡単に構成できる。このような専用のハードウェアデコーダを有するコンピュータシステムの構成例を図6に示す。

【0027】このシステムはデスクトップ型パーソナルコンピュータに対応するものであり、図示のように、PCIバス10、CPU11、主メモリ(MEM)12、HDD13、ATAPIまたはSCSIインタフェースから構成されるDVDインターフェース16、オーディオコントローラ17、DVDデコーダ18、マルチメディアディスプレイコントローラ19、およびビデオメモリ(VRAM)20を備えており、MPEG2によって符号化された動画データなどを格納したDVD-ROMドライブ21は、DVDインターフェース16に接続されている。

【0028】CPU11は、このシステム全体の動作を制御するものであり、システムメモリ(MEM)12に格納されたオペレーティングシステムおよび実行対象のアプリケーションプログラムを実行する。DVD-ROMドライブ21に記録されたデータの転送及び再生は、CPU11にDVD制御ドライバを実行させることによって実行される。

【0029】DVDインタフェース16は、HDDやCD-ROMなどのディスク装置をPCIバス10に接続するためのディスクインタフェースであり、この実施形態では、CPU11からの指示に従いDVD-ROMドライブ21との間のデータ転送を行う。オーディオコントローラ17は、CPU11の制御の下にサウンドデータの入出力制御を行うものであり、サウンド出力のために、PCM音源171、FM音源172、マルチプレクサ173、およびD/Aコンバータ174を備えている。マルチプレクサ173には、PCM音源171お

よびFM音源172からの出力と、DVDデコーダ18から転送されるデジタルオーディオデータが入力され、それらの1つが選択される。

【0030】デジタルオーディオデータは、DVD-ROMドライブ21から読み出されたオーディオデータをデコードしたものである。DVDデコーダ18からオーディオコントローラ17へのデジタルオーディオデータの転送には、オーディオバス18aが用いられ、PCIバス10は使用されない。従って、コンピュータシステムの性能に影響を与えることなくデジタルオーディオデータの高速転送が可能となる。

【0031】DVDデコーダ18は、CPU11の制御の下に、DVDインターフェース16からMPEG2プログラムストリームを読み出し、それをビデオ、サブピクチャ、およびオーディオパケットに分離した後、それらをそれぞれデコード処理し同期化して出力する。このDVDデコーダ18は、例えばこのコンピュータシステムのPCI拡張スロットに取り外し自在に装着できるPCI拡張カードとして実現されており、図示のように、マスタランザクション制御部201、ディスクランブル制御部202、MPEG2デコーダ203が設けられている。

【0032】マスタランザクション制御部201は、DVDデコーダ18をPCIバス10上にランザクションを発行するバスマスタ(イニシエータ)として動作させるためのものであり、DVDインターフェース16から動画データを読み出すためのI/Oリードランザクションを実行する。マスタランザクション制御部201によって読みとられたMPEG2プログラムストリームは、ディスクランブル制御部202でIピクチャについてのディスクランブルが行われた後、MPEG2デコーダ203に送られる。MPEG2デコーダ203では、MPEG2プログラムストリームからビデオ、サブピクチャ、およびオーディオパケットへの分離処理と、それらのデコード処理が行われる。

【0033】デコードされたオーディオデータは、前述したようにデジタルオーディオデータとしてオーディオバス18aを介してオーディオコントローラ18aに転送される。デコードされたビデオおよびサブピクチャは合成されて、デジタルYUVデータとしてマルチメディアディスプレイコントローラ19に送られる。この場合、DVDデコーダ18からマルチメディアディスプレイコントローラ19へのデジタルYUVデータの転送には、ビデオバス18bが用いられ、PCIバス10は使用されない。従って、デジタルYUVデータの転送についても、デジタルオーディオデータと同様に、コンピュータシステムの性能に影響を与えることなく高速に行うことができる。

【0034】ビデオバス18bとしては、VESA規格のVAFC(VESA Advanced Featu

re Connector)、またはVM-Channel (VESA Media Channel) を利用することができる。

【0035】また、DVDデコーダ18は、デジタルYUVデータとオーディオデータをNTSC方式のTV信号に変換してTV受像機の外部ビデオ入力に出力する機能も有している。DVDデコーダ18からTV受像機へのTV信号の送信は、DVDデコーダ18のカードに設けられたコネクタに、TV受像機への導出ケーブルを接続することによって容易に行うことができる。

【0036】マルチメディアディスプレイコントローラ19は、CPU11の制御の下に、このシステムのディスプレイモニタとして使用されるCRTディスプレイを制御するものであり、VGA仕様のテキストおよびグラフィックス表示の他、動画表示をサポートする。

【0037】このマルチメディアディスプレイコントローラ19には、図示のように、グラフィックス表示制御回路(Graphics)191、ビデオ表示制御回路192、マルチプレクサ193、およびD/Aコンバータ194等が設けられている。

【0038】グラフィックス表示制御回路191は、VGA互換のグラフィックスコントローラであり、ビデオメモリ(VRAM)20に描画されたVGAのグラフィックスデータをRGBビデオデータに変換して出力する。ビデオ表示制御回路192は、デジタルYUVデータを貯えるビデオバッファ、及び同バッファに貯えられたYUBデータをRGBビデオデータに変換するYUB-RGB変換回路等をもつ。

【0039】マルチプレクサ193は、グラフィックス表示制御回路191とビデオ表示制御回路192の出力データの一方を選択、またはグラフィックス表示制御回路191からのVGAグラフィックス上にビデオ表示制御回路192からのビデオ出力を合成してD/Aコンバータ194に送る。D/Aコンバータ194は、マルチプレクサ194からのビデオデータをアナログRGB信号

に変換して、CRTディスプレイに出力する。

【0040】

【発明の効果】以上説明したように、この発明によれば、動画データの一部のみを暗号化することでその動画データの表示再生などの不正使用を防止できるようになり、コピープロテクト機能とソフトウェアデコーダとを同時に満足させることが可能となる。

【図面の簡単な説明】

【図1】この発明の一実施形態に係るコンピュータシステムで使用されるソフトウェアデコーダの機能構成を示すブロック図。

【図2】同実施形態で使用される動画データストリームのデータ構造を示す図。

【図3】同実施形態で使用されるスクランブルルールの情報の格納位置を示す図。

【図4】同実施形態で使用される符号化装置の構成を示すブロック図。

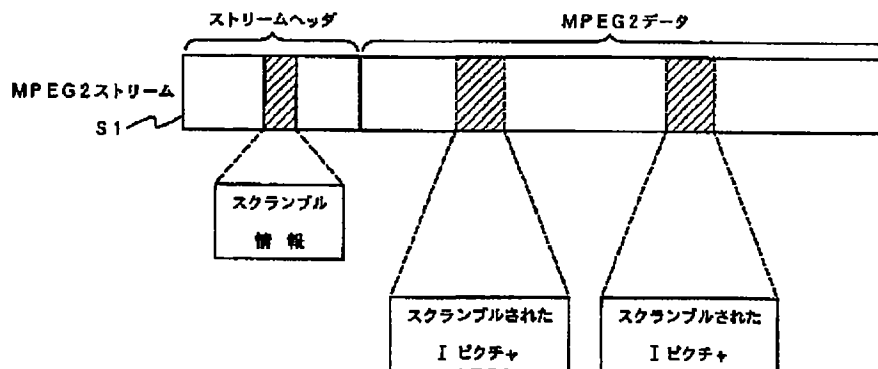
【図5】同実施形態における動画再生処理の手順を示すフローチャート。

【図6】同実施形態のシステムのハードウェア構成を示すブロック図。

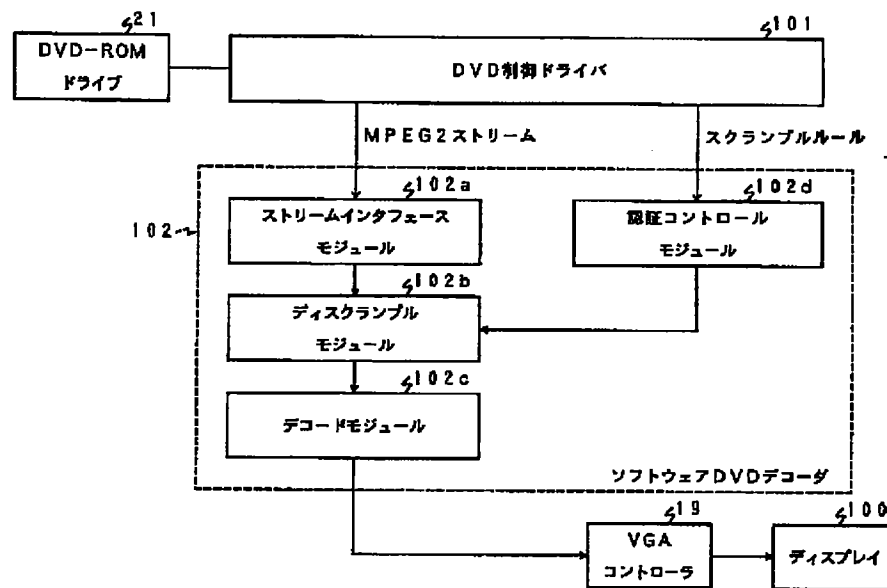
【符号の説明】

101…DVD制御ドライバ、102…ソフトウェアDVDデコーダ、102a…ストリームインタフェースモジュール、102b…ディスクランブルモジュール、102c…デコードモジュール、102d…認証モジュール、10…システムバス、11…CPU、12…システムメモリ、16…ATAPIインタフェース、17…オーディオコントローラ、18…DVDデコーダ、19…マルチメディアディスプレイコントローラ、20…ビデオメモリ、21…DVD-ROMドライブ、161…I/Oポート、201…マスタートランザクション制御部、202…ディスクランブル制御部、203…MPEG2デコーダ。

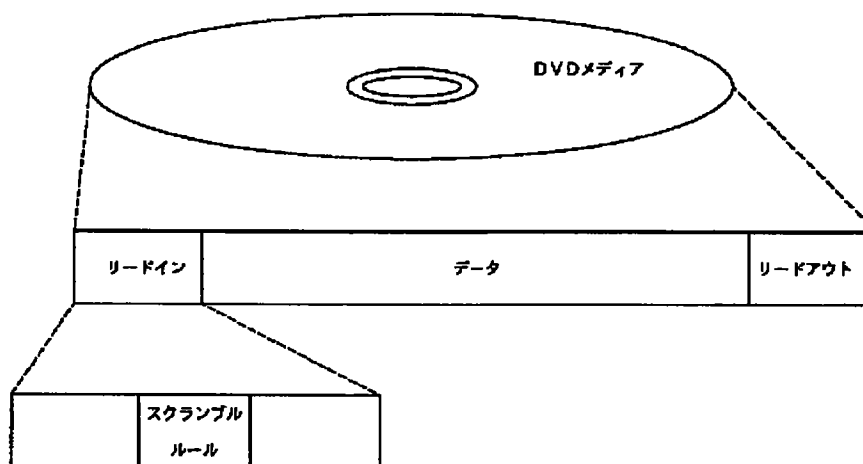
【図2】



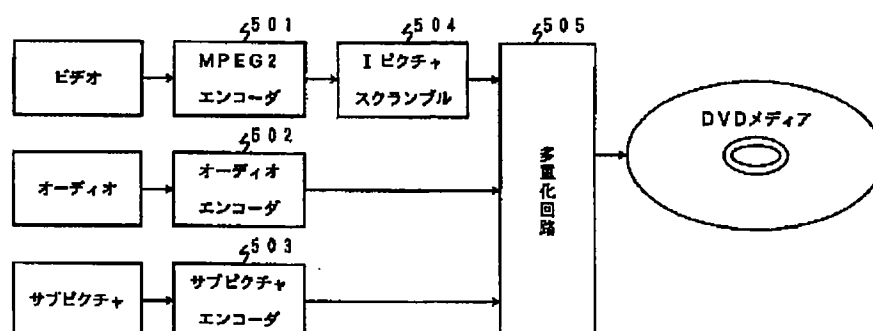
【図1】



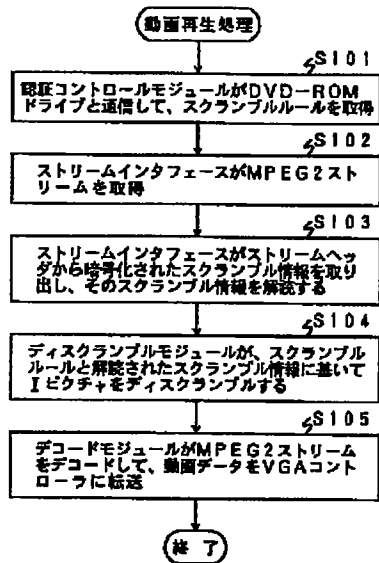
【図3】



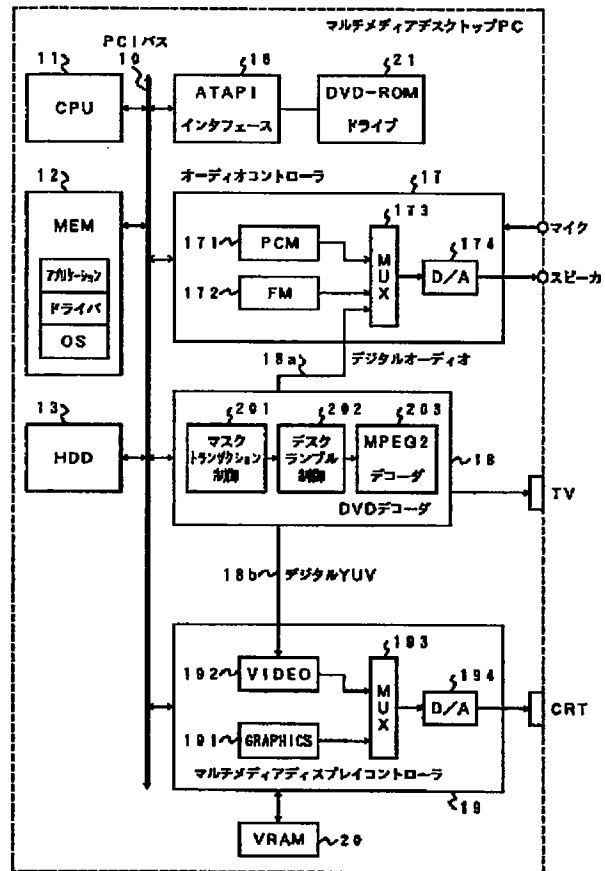
【図4】



【図5】



【図6】



(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-342246

(P2004-342246A)

(43) 公開日 平成16年12月2日(2004.12.2)

(51) Int. Cl.⁷

F I

テーマコード (参考)

G 1 1 B 20/10

G 1 1 B 20/10

H

5 B 0 1 7

G 0 6 F 12/14

G 0 6 F 12/14

3 2 O B

5 D 0 4 4

G 1 1 B 20/12

G 0 6 F 12/14

3 2 O E

5 D 1 1 0

G 1 1 B 27/00

G 0 6 F 12/14

3 2 O F

5 J 1 0 4

H 0 4 L 9/08

G 1 1 B 20/12

審査請求 未請求 請求項の数 28 O L (全 46 頁) 最終頁に続く

(21) 出願番号 特願2003-138551 (P2003-138551)

(22) 出願日 平成15年5月16日 (2003.5.16)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(74) 代理人 100093241

弁理士 宮田 正昭

(74) 代理人 100101801

弁理士 山田 英治

(74) 代理人 100086531

弁理士 澤田 俊夫

(72) 発明者 木谷 聡

東京都品川区北品川6丁目7番35号 ソ

ニー株式会社内

(72) 発明者 浅野 智之

東京都品川区北品川6丁目7番35号 ソ

ニー株式会社内

最終頁に続く

(54) 【発明の名称】 情報処理装置、情報記録媒体、コンテンツ管理システム、および方法、並びにコンピュータ・プログラム

(57) 【要約】

【課題】 情報記録媒体に格納される暗号化コンテンツの不正利用の防止、不正複製についての情報漏えいルート解析を可能とした構成を提供する。

【解決手段】 コンテンツ編集エンティティが、記録シード (REC SEED) を生成し、管理センタから受領する鍵情報、および鍵生成情報 (第2シード) に基づいて第2ブロックキー K b 2 を生成し、第2ブロックキー K b 2 に基づくコンテンツ暗号化を実行する。情報記録媒体製造エンティティが、物理インデックスを生成し、管理センタから受領する鍵情報、および鍵生成情報 (第1シード) に基づいてブロックキー K b 1 を生成し、生成した第1ブロックキー K b 1 に基づく第2シードの暗号化を実行し、これらの情報および各エンティティのコード情報を情報記録媒体に格納する。

【選択図】 図18

